

administrative expenses for work associated with the contract.

Pension costs. The FEHBP is charged a certain percentage to cover pension costs for plan employees who work on FEHBP activities. When a plan reduces its workforce and therefore its overall pension costs, it should make a corresponding reduction to the FEHBP's allocation for pension costs.

Although the plan reduced its workforce, it did not adjust the pension costs charged to the FEHBP in contract years 1998 and 1999. Therefore, our auditors calculated that the plan overcharged the FEHBP \$149,644 for pension costs in those years. We recommended that the contracting officer instruct the plan to credit the FEHBP for these pension cost overcharges.

Cash Management

Regarding cash management of FEHBP funds, our auditors concluded that Anthem had handled these funds from 1997 through 1999 in accordance with applicable laws and regulations with one exception. The exception occurred during December 1997 when the plan did not credit the FEHBP \$3,181 for investment income.

Lost Investment Income

Federal regulations require a carrier to invest and reinvest all excess FEHBP funds on hand and to credit all investment income earned on those funds. We computed lost investment income resulting from our audit findings in the amount of \$36,726 through June 30, 2001. We have recommended to the contracting officer that lost investment income of \$36,726 be returned to the FEHBP, as well as additional lost investment income due after that date until Anthem has returned all questioned costs owed to the FEHBP.

BlueCross BlueShield of New Mexico

in Albuquerque, New Mexico

Report No. 1A-10-03-01-027
July 25, 2001

Our audit of the FEHBP operations at BlueCross BlueShield of New Mexico (BCBS of New Mexico) took place at the plan's headquarters in Albuquerque, New Mexico. We reviewed health benefit payments made by the plan from 1997 through 1999, as well as miscellaneous payments and administrative expenses for contract years 1995 through 1999.

In performing this audit, we determined whether the plan charged costs to the FEHBP and provided services to FEHBP members in accordance with the terms of its contract. At the conclusion of this audit, our auditors determined that the plan improperly charged the FEHBP \$816,101 in claim payments and never credited the FEHBP \$2,428 for a refund. Lost investment income on these questioned amounts totaled \$328. Final calculations by our auditors regarding all inappropriate charges and lost investment income to the FEHBP totaled \$818,857. The BCBS Association agreed with all the questioned amounts.

Health Benefits

From 1997 through 1999, BCBS of New Mexico paid \$109 million in actual FEHBP claim payments. We selected claims to examine at random and in specific health benefit categories. Principally, these concerned coordinating benefits with Medicare and potential duplicate payments. We also reviewed specific financial and accounting areas, such as refunds and other miscellaneous

Auditors
Calculate
**\$818,857 Owed
to the FEHBP**

credits relating to FEHBP claim payments. Our findings related only to health benefit charges and totaled \$818,857. Some of our findings in this area were:

Coordination of benefits. During this review, we identified 949 claim payments where the FEHBP paid as primary insurer when Medicare Part A or B was actually the primary insurer. As a result, we estimated that the plan overcharged the FEHBP \$732,237 for these coordination of benefit payment errors.

As discussed in the preceding audit narrative on the Anthem BCBS plan, this type of inappropriate charge occurs when there is a failure to coordinate benefits properly with Medicare coverage. To assist its BCBS member plans with this and other claim reviews, the BlueCross BlueShield Association maintains a national claims system database at its Federal Employee Program (FEP) operations center in the Washington, D.C. area.

For most of the claim lines questioned, there was no information in the BCBS Association national database to make the plan aware that Medicare benefits coordination was necessary at the time these claims were paid. However, when this Medicare information was later added to the FEP claims system, BCBS of New Mexico did not review and adjust its members' prior claim lines back to the Medicare effective dates. Therefore, the claim benefit costs remained charged to the FEHBP in their entirety, which resulted in overcharges of \$732,237 to the FEHBP.

These claims involved Medicare Parts A and B. Similarly, BCBS of New Mexico did not follow its procedures and coordinate inpatient claims when patients had Medicare Part B only. We recommended that OPM's contracting officer disallow all of these uncoordinated claim payments and instruct the plan to make every reasonable effort to recover

these overpayments and credit all amounts recovered to the FEHBP.

Duplicate claim payments. BCBS of New Mexico inappropriately charged the FEHBP for duplicate claim payments during contract years 1997 through 1999. Of the approximately \$109 million in claims paid during this period, our auditors identified 159 duplicate claim payments, totaling \$83,864. Having noted that this was a small number of duplicate claim payments, we concluded that the plan had effective controls in place to minimize such payments.

Refunds. In one instance, BCBS of New Mexico did not credit the FEHBP for a refund of \$2,428 it received in 1999. Federal regulations require the carrier to credit refunds relating to health benefit payments to the FEHBP, along with investment income lost on these funds. Consequently, our auditors determined that BCBS of New Mexico owed the FEHBP \$328 in lost investment income on this refund. As a result, we recommended that the contracting officer ensure that the plan credits the FEHBP \$2,756 representing the refund and associated lost investment income.

Administrative Expenses

For contract years 1995 through 1999, BCBS of New Mexico charged the FEHBP \$16.3 million in administrative expenses. Our auditors determined that the administrative expenses incurred and charged to the FEHBP were actual, necessary, and reasonable expenses incurred in accordance with the terms of the contract and applicable regulations.

Experience-Rated Comprehensive Medical Plans

Comprehensive medical plans (HMOs) fall into one of two categories: community-rated or experience-rated. As was previously explained in more detail on page 5 of this section, the critical differ-

Uncoordinated
Medicare
Payments Cost
FEHBP \$732,237

ence between the two categories stems from how premium rates are calculated for each.

Like other health insurance plans participating in the FEHBP, experience-rated HMOs offer what is termed a “point of service” product. Under this option, members have the choice of using a designated network of providers or using non-network providers.

In selecting one health provider over another, a member’s choice has specific monetary and medical implications. For example, if a member chooses a non-network provider, the member will pay a substantial portion of the charges and the benefits available may be less comprehensive.

During this reporting period, we issued one experience-rated comprehensive medical plan draft audit report but no final reports.

Employee Organization Plans

Employee organization plans also fall into the category of experience-rated, and may operate or sponsor participating health benefits programs.

The two largest types of employee organizations are federal employee unions and associations. Some examples are the American Postal Workers Union, the National Association of Letter Carriers, the Government Employees Hospital Association and the Special Agents Mutual Benefit Association. These plans operate on a fee-for-service basis, which allows members to obtain treatment through facilities or providers of their choice.

We did not issue any final reports for employee organization plans during the reporting period.

Information Systems Audits

In accordance with the Inspector General Act of 1978, as amended, we conduct and supervise independent and objective audits of agency programs and operations to prevent and detect fraud, waste and abuse. To assist in fulfilling this mission, we perform information systems audits of health and life insurance carriers that participate in the Federal Employees Health Benefits Program (FEHBP) and the Federal Employees' Group Life Insurance program (FGLI). We also audit the agency's computer systems development and management activities.

Information systems audits are a relatively new audit activity for our OIG. We are pleased with our early success in auditing computer information systems of health insurance carriers participating in the Federal Employees Health Benefits Program (FEHBP). We have had similar results in detecting control weaknesses in reviewing OPM's internal information systems control environment.

The inherent need for this type of oversight lies in the federal government's heavy reliance on information systems to administer federal programs, manage federal resources, and accurately report costs and benefits. Any breakdown in federal computer systems, including systems of federal contractors, can compromise the government's efficiency and effectiveness, increase the costs of federal projects and programs, and threaten the safety of United States citizens.

Ever increasing malicious attacks on both public and private computer systems underscore the importance of this issue. These threats include outbreaks of destructive computer viruses, web site defacements, sabotage, and theft of valuable or sensitive information in computer databases.

To minimize information system security risks, our office audits various agency

computer systems development and security-related activities. In addition, our office conducts audits pertaining to general and applications controls at health carriers under contract with OPM to provide health benefits under the FEHBP.

General controls are defined as the policies and procedures that apply to an entity's overall computing environment. *Application controls* are those directly related to individual computer applications, such as a carrier's payroll system or benefits payment system. General controls provide a secure setting in which computer systems can operate, while application controls ensure that the systems completely and accurately process transactions.

During this reporting period, we completed an evaluation of OPM's security programs and practices in accordance with Title X, Subtitle G ("Government Information Security Reform") contained in P.L. 106-398, the FY 2001 Defense Authorization Act. We also completed an audit of an FEHBP carrier's information systems general controls and a review of OPM's Internet privacy practices. A summary of our audit findings and recommendations are described on the following pages.

Review of OPM's Compliance With the Government Information Security Reform Act

Report No. 4A-CI-00-01-088
August 31, 2001

On October 30, 2000, former President Clinton signed into law the FY 2001 Defense Authorization Act that included an important amendment to the Paperwork Reduction Act of 1995 pertaining to information security.

This subchapter of the FY 2001 Defense Authorization Act is commonly referred to as the Security Act. It focuses on program management, implementation and evaluation of security for unclassified and national security computer systems, and seeks to ensure proper management and security for the information resources supporting federal operations and assets.

General Overview

Pursuant to the Security Act, we performed an independent evaluation of OPM's computer security program and practices. We evaluated OPM's entity-wide security controls and the security environment of the mainframe computer operation. This computer operation supports most of OPM's essential systems, including critical applications for the agency's Retirement and Insurance Service, Investigations Service, and Office of the Chief Financial Officer.

In addition, we reviewed OPM's general compliance efforts for specific areas defined in the U.S. Office of Management and Budget's (OMB) Security Act implementation guidance and corresponding reporting instructions.

While we concluded that OPM is committed to improving its computer security, we identified several areas where progress is still needed. However, nothing came to our attention that would cause us to believe that there are material weaknesses in OPM's information security controls. The specifics of our review are summarized below.

Security Program Performance

Program office compliance. OPM maintains a security plan for the mainframe operation and assets under its control. Also, security personnel have appropriately configured the security software to maintain an audit trail of system activity and ensure that security violations are reported to management and subsequently investigated. However, we determined that OPM's mainframe systems administrator does not have a formal methodology to assess the risks associated with the operations and assets under the administrator's control.

OCIO security responsibilities. OPM has not yet implemented an agency-wide security program. However, a draft information technology security policy has been developed by OPM's Office of the Chief Information Officer (OCIO).

Security training. OCIO has not implemented a security training program to ensure that employees are sufficiently trained in their security responsibilities. While several key staff members have received some technical training, most have not. However, OCIO has sponsored security awareness training for all agency employees and contractors the last two years. This fall, OCIO is planning a comprehensive, online security awareness program.

 **OPM
Committed
to Improving
Computer
Security**

Weaknesses Noted in OPM's Computer Security Program

Incident reporting. OPM does not have a documented, formally established computer incident response team. The absence of this team could cause existing or potential vulnerabilities to escape detection.

Capital planning. OPM has not adequately integrated security requirements or cost estimates into its capital planning and investment control process.

Critical assets planning strategies. OPM has implemented controls to identify, prioritize, and protect critical assets within its enterprise architecture. The strategies used by OPM include developing and testing a draft disaster recovery plan for its mainframe operation and implementing an agency-wide continuity of operations plan.

Security life cycle. Although OPM has not completed the development of an agency-wide systems development life cycle (SDLC) methodology, it has made significant progress toward that goal. OPM has established an SDLC framework and has started to implement pieces of it. Implementing this strategy will ensure that information technology security will be included as an important aspect of future system development efforts at OPM.

Critical infrastructure protection. OPM is not in compliance with directives on critical infrastructure protection. This issue was discussed in detail in our April 2001 semiannual report to Congress.

Contractor services security. Contractors employed by OPM are supervised in accordance with OPM regulations. Contractors have unique user identifications for accountability, reporting and monitoring purposes. However, we found that OPM does not have adequate controls for deleting system access for contractors when they leave the agency.

OPM Specific Security Act Responsibilities

We determined that OPM was not in compliance with two of the three government-wide training responsibilities identified in the Security Act.

Specifically, OPM has not reviewed or updated regulations concerning computer security training for federal civilian employees. OPM also has not assisted the Department of Commerce in updating and maintaining guidelines for training in computer security awareness and computer security best practices. However, OPM has worked with the National Science Foundation to develop and implement a Scholarship for Service (SFS) program to promote the development of information technology skills within the federal government. This program provides scholarships to undergraduate and graduate students who are pursuing a degree in the information assurance and computer security fields. It is set to begin this fall.

OPM Internet Privacy Review

Report No. 4A-CI-00-01-038
May 9, 2001

Last year, Congress passed the Treasury and General Government Appropriations Act of 2001, Public Law 106-544. Contained in section 646 of this act is a directive to the Inspector General of each department or agency to submit to Congress a report that discloses any agency activity related to the collection or review of personally identifiable information from individuals who access the agency's Internet sites.

It also requires the disclosure of any agreements with third parties to collect, review or obtain personally identifiable information relating to an individual's access or viewing habits for governmental and non-governmental Internet sites.

In accordance with P.L. 106-544, we conducted a review to determine whether OPM, or any third parties under agreement with OPM, are obtaining personally identifiable information relating to any individual's access or viewing habits without appropriate authorization.

We determined that OPM is not collecting personally identifiable information on OPM Internet users' access or viewing habits through its web sites or through third-party agreements. However, we did identify several areas where the agency could improve its Internet web site practices.

We have recommended that the Office of the Chief Information Officer, who maintains responsibility for OPM's Internet activities, do the following:

- Implement steps to ensure that all major entry points into OPM's web sites and any OPM web pages, where substantial amounts of personal information is collected, have a direct link to OPM's privacy policy.
- Continue to work with program offices to ensure that OPM web sites do not use persistent cookies to collect personally identifiable information, as directed in OPM's privacy policy. *Persistent cookies* are small bits of software placed on a web user's hard drive that can be used to track web browsing behavior.

- Review and update the agency's policies and procedures relating to Internet web site activity.

Regarding the last bulleted recommendation, our office has suggested that these improvements include the following:

- Adding a section to its policies and procedures related to agency and program office Internet privacy responsibilities.
- Updating a web page approval process.
- Implementing formal change control policies and procedures related to web site development and maintenance.
- Adding a section that addresses agreements with third parties for web site activities.
- Requiring all OPM web sites with non-OPM hyperlinks to notify the user when they are about to leave an OPM web site.

The Chief Information Officer stated that her office concurs with our findings, conclusions and recommendations. OCIO has concluded through its own review and a concurrent internal review that the agency needs to adopt a more formal and rigorous process related to Internet web site activities.

As an initial step, they have already obtained agency-wide management approval to reengineer how they will accomplish this work. OCIO also plans to incorporate our recommendations into the development and implementation of its updated Internet web site policies and procedures.

Auditors Recommend Improvements in OPM's Web Site Practices

PM Management Agrees with Web Site Security Recommendations

***Audit of Information
System General Controls
at the BlueCross
BlueShield Association
FEP Operations Center
in Washington, D.C.***

Report No. 1A-10-92-00-028
July 30, 2001

The goal of our audit was to obtain reasonable assurance that the operations center had implemented proper controls over the integrity, confidentiality and availability of computerized data associated with is FEHBP contracts. We evaluated the plan's information system general controls using guidance contained in the General Accounting Office's *Federal Information System Controls Audit Manual*, industry best practices, along with pertinent federal law and regulations.

This review included examining how well CareFirst was managing security policy and access controls, along with software changes related to CareFirst's information systems. Our auditors also assessed whether there was an appropriate segregation of duties among employees who were involved in the FEP operations center's information systems. Additionally, we looked at controls over the mainframe operating system and examined the operations center's plan for maintaining or quickly restoring all its computer systems functions in the event of a disaster.

Our audit revealed that the FEP operations center managers should take steps to strengthen and formally implement a corporate security plan. We also found that there were opportunities for improvement in other general controls that had been implemented at the operations center to safeguard its assets and data. As a result, our auditors made a number of recommendations intended to improve those controls.

In response, FEP operations center management agreed to implementing many of our recommendations, beginning with updating, revising and consolidating its security policies and procedures.

The BlueCross and BlueShield Association (BCBS Association) contracts with our agency on behalf of its numerous member plans. Participating Blue Cross and Blue Shield plans throughout the United States underwrite and process the health benefits claims of their respective federal subscribers under the government-wide BCBS Service Benefit Plan. Approximately 46 percent of all FEHBP subscribers are enrolled in Blue Cross and Blue Shield plans nationwide.

Because of the sheer number of federal subscribers served by BCBS member plans, we considered this audit of the association's Federal Employee Program (FEP) operations center particularly important. During FEHBP contract year 2000, which was the scope of our audit, the operations center processed \$6.3 billion in FEHBP claims.

The FEP operations center is the central processing location for all medical claims processed by the various Blue Cross and Blue Shield plans. Currently, the BCBS Association contracts with CareFirst BlueCross BlueShield to host and maintain the operations center at its Columbia, Maryland data center in suburban Washington, D.C.

**Computer
Operations
at BCBS Central
Processing Center
Benefit from
Audit
Recommendations**

In other general controls areas, the operations center has accepted our recommendations to improve policies and procedures related to application software development, application change control, and system software. For example, the operations center managers have assigned a team to improve and implement procedures to control changes to application software. In addition, operations center management is developing formal written procedures to initiate,

approve and review changes to critical operating system data sets.

We believe that our review, and particularly our specific recommendations, will enhance the BCBS Association FEP operations center's information system general controls, thereby safeguarding the confidential medical records of the association's FEHBP enrollees, as well as ensuring the reliability and continued availability of the operations center's critical automated information.

Other External Audits

When requested by Office of Personnel Management (OPM) procurement officials, our office conducts pre- and post-award contract audits relating to the acquisition of goods and services by agency program offices. We also conduct audits of the local organizations of the Combined Federal Campaign (CFC), the only authorized fundraising drive conducted in federal installations throughout the world.

Combined Federal Campaign

The U.S. Civil Service Commission (the precursor of OPM) was given the responsibility of arranging for national voluntary health and welfare agencies to solicit funds from federal employees and members of the armed services at their place of employment by Executive Order 10927, issued on March 18, 1961. Since then, additional executive orders and new federal regulations (5 CFR 950) have been issued as well as one public law (P.L. 100-202) that:

- Make national and local organizations and charities eligible to participate in the Combined Federal Campaign (CFC).
- Define the role of local CFC organizations.
- Cite OPM's oversight responsibilities regarding the Combined Federal Campaign.

An estimated 366 local campaigns participated in the 2000 Combined Federal Campaign, the most recent year for which statistical data is available. These CFCs are usually organized within large urban areas to maximize the territory covered where federal employees work and live. Federal employee contributions reached \$224 million for the 2000 CFC, while administrative expenses totaled \$19.4 million.

Combined Federal Campaign audits will not ordinarily identify savings to the government, because the funds involved are charitable donations made by federal employees, not federal entities. While infrequent, our audit efforts can result in an internal referral to our OIG investigators for potential fraudulent activity.

During the current reporting period, we issued 11 final CFC reports, a listing of which is on page 47 in Appendix VI.

As described in previous semiannual reports, our CFC audits have focused on the eligibility of local charities participating in local campaigns, on local campaign compliance with CFC regulations, and testing the various local campaigns' financial records. This year's audits covered campaign years 1998 and 1999.

CFC Audit Findings

Generally speaking, the local CFC administrators we audited were in compliance with federal regulations and guidelines. However, we found some key noncompliances. These noncompliances described below were taken from two of our CFC audits to illustrate those areas in which the CFC administrators needed to improve when conducting future campaigns.

These CFC administrators failed to:

- Follow proper application procedures.
- Notify charities of their eligibility status within established time frames.

Auditors Note Areas of Noncompliance with CFC Regulations & Guidelines

- Adhere to regulations regarding administrative expense reimbursements.
- Accurately identify a charity in a local campaign brochure.
- Distribute donations within required time limits.
- Provide timely responses to OIG auditor requests.

Agency Contract Audits

Our office conducts two types of agency contract audits. We perform pre-award contract audits to: (1) ensure that a bidding contractor is capable of meeting contractual requirements; (2) assess whether estimated costs are realistic and reasonable; and (3) determine if the

contract complies with all applicable federal regulations. We also conduct post-award contract audits to ensure that costs claimed to have been incurred under the terms of an existing contract are accurate and in accordance with provisions of federal contract regulations.

These audits provide OPM procurement officials with the best information available for use in contract negotiations and oversight. In the case of post-award contract audits, for example, the verification of actual costs and performance charges may be useful in negotiating future contract modifications pertaining to cost-savings and efficiency.

During this reporting period, we did not issue any audit reports on agency contracts.

OPM Internal Audits

Our office is responsible for conducting audits, as well as evaluations and inspections, of the Office of Personnel Management's (OPM) programs and administrative operations. This includes audits of OPM's consolidated financial statements required under the Chief Financial Officers Act (CFO Act of 1990) and performance reviews, particularly those pertaining to the human resource management role OPM fulfills for the federal government.

Our internal audits staff consists of auditors and program evaluators working together to provide recommendations for improving the economy and efficiency of our agency operations. We use a risk-based methodology to assess OPM's activities and establish annual work agendas. The objective is to identify high impact areas where the OIG can provide the best possible benefit to the agency.

To ensure that we achieve our goals, we carefully plan and conduct our activities involving audits or evaluations and inspections in accordance with government standards. We conscientiously include OPM program managers in every step of the audit process to ensure that we have met their needs, addressed concerns and obtained feedback on how we can improve the value of our services. We believe this cooperative spirit ensures that all parties involved with our activities will obtain the maximum benefit and that we will continually improve our level of services.

During this reporting period, we: (1) completed one internal audit of OPM's FY 2000 annual performance report; (2) addressed one congressional inquiry relating to OPM's 12 most significant performance measures (indicators) and another concerning improper payments made from the retirement, health and life insurance trust funds administered by the agency; and (3) continued our

assistance to the Office of the Chief Financial Officer (OCFO). We also issued a report on OMB Bulletin 01-02 concerning OPM's benefit withholdings and contributions payroll procedures.

The following pages contain descriptions of our efforts in each of these areas and an update on OPM management's top ten challenges as identified by our OIG.

Performance Audits

During this reporting period, we continued to concentrate our performance audit efforts on agency program audits. As defined by Government Auditing Standards, a *program audit* can determine three things:

- The extent to which the desired results or benefits established by the U.S. Congress or another authorizing body are being achieved.
- The effectiveness of programs, activities or functions.
- Agency compliance with significant laws and regulations.

Specifically, we reviewed documentation relating to our agency's data prepared under the requirements of the Government Performance and Results Act of 1993. This act, most frequently referenced by its acronym GPRA, was designed to produce improvements in government performance and account-

ability in federal programs. GPRA also includes directives for federal agencies and departments to follow regarding strategic planning and performance management processes that emphasize goal-setting, customer satisfaction and results measurements.

In an October 1998 congressional request, the IG community was asked to include in future semiannual reports to Congress a summary of reportable actions under GPRA resulting from OIG audit activities. Accordingly, the following paragraphs describe these activities and corresponding results.

Audit of Internal Controls of OPM's FY 2000 Performance Results

Report No. 4A-OP-00-01-023
June 19, 2001

Verification and validation reviews. The Government Performance and Results Act of 1993 requires agencies to prepare an annual performance plan covering each program activity. GPRA also instructs agencies to instruct a description of the means to be used to verify and validate measured values. The U.S. General Accounting Office's (GAO) report, titled *Selected Approaches for Verification and Validation of Agency Performance Information* (GAO/GGD-99-139), defines verification and validation as follows:

- *Verification* is the assessment of data completeness, accuracy, consistency, timeliness and related quality control practices.
- *Validation* is the assessment of whether data are appropriate for the performance measure.

Although not required under GPRA, we decided to perform our own verification and validation reviews to assess independently OPM's performance required under GPRA. Our decision was based on the high level of interest afforded GPRA by Congress and the GAO.

The objectives of our reviews were to:

- Verify and validate performance data for selected FY 2000 GPRA performance indicators in OPM's performance report.
- Evaluate the effectiveness of controls over performance measurement data.

Our agency submitted its second annual performance plan to Congress with its FY 2000 budget request. The performance plan established five general agency goals, 117 program goals and 458 performance indicators (measures). Out of those goals and measures, we focused on eight major program offices by selecting 42 program goals and 117 performance measures to verify and validate.

Specifically, we selected goals and performance measures from the following OPM program offices:

- Office of Executive and Management Development
- Investigations Service
- Employment Service
- Office of Merit Systems Oversight and Effectiveness
- Retirement and Insurance Service
- Office of the Chief Financial Officer
- Office of Workforce Relations
- Workforce Compensation and Performance Service

IG Conducts Reviews of OPM Performance Data

Controls Over Agency Performance Reporting Need Strengthening

Included in our selection were many of the goals that relate to the top management issues we reported to members of the House and Senate in letters dated December 1, 2000 (see table on page 31), and referenced in our last two OIG semi-annual reports.

At the completion of our reviews, we found that OPM specifically needed to improve controls over the performance reporting process. We noted the following areas within OPM program operations that needed to be addressed and improved:

- Establishing policies and procedures for obtaining and compiling performance data.
- Providing better oversight and monitoring of performance data by OPM managers.
- Improving documentation supporting performance data.
- Using specific time frames (cutoff controls) to coincide with performance data.
- Correlating results to pertinent measures.

Our office is encouraged that OPM management has been responsive to our findings and has begun taking steps to implement improvements.

To put our findings in their proper context, we recognize that performance reporting is still a new process for all federal departments and agencies. We also realize that additional guidance will be forthcoming from Congress and the Office of Management and Budget through our agency's budget review process. In the interim, we can report with confidence that OPM remains committed to presenting accurate and consistent data in meeting GPRA requirements.

While not all other OPM program offices had the same issues described in the preceding bullets, all of these deficiencies point to the need for OPM's performance results to be as accurate and reliable as possible. We will continue our oversight of our agency's performance measurement reporting through our OIG's annual verification and validation reviews.

OIG Responds to Congressional Leadership Inquiries

As with all OIGs, we receive many requests from Congress, particularly from the Senate and House leadership and from those committees having jurisdiction over our respective agency programs. A number of these inquiries have fallen under the purview of our internal audit activities that we believe are noteworthy.

In the immediate paragraphs that follow, we describe three inquiries received during the current reporting period we consider of particular importance. One relates to OPM's performance and accountability report and another to improper payments made from the three federal benefits programs (retirement, health and life) administered by our agency. In the third inquiry, we were asked to provide updates on the status of OPM's top management challenges our OIG had identified in a previous reporting period.

The critical aspects of our response to these inquiries are highlighted below.

OPM's FY 2000 Performance & Accountability Report

On April 5, 2001, the Honorable Dan Burton, in his capacity as chairman of the House Committee on Government Reform, asked our office to review

OPM Management Committed to Improving Performance Reporting